

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-237484

(43)Date of publication of application : 23.08.1994

(51)Int.Cl.

H04Q 7/04

(21)Application number : 03-126287

(71)Applicant : FR TELECOM

(22)Date of filing : 29.05.1991

(72)Inventor : LANGRAND FRANCK
MAZZIOTTO GERALD
BAUDOUX SOPHIE

(30)Priority

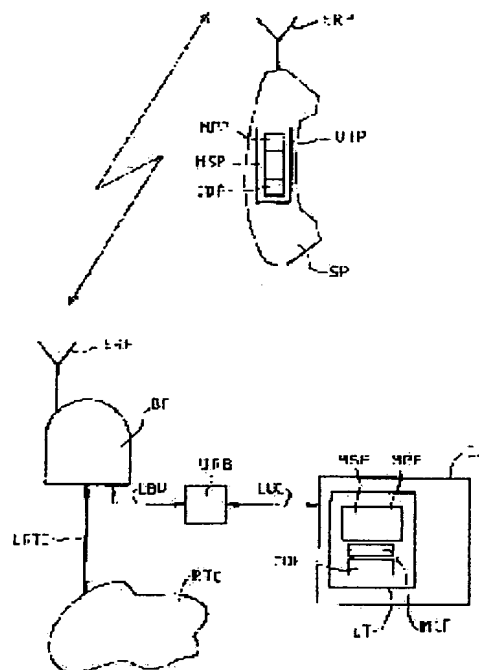
Priority number : 90 9006662 Priority date : 29.05.1990 Priority country : FR

(54) TELEPHONE SYSTEM FOR REMOTELY LOADING TELEPHONE SUBSCRIPTION DATA OF ISOLATED STATION

(57)Abstract:

PURPOSE: To obtain a device and method having high safety with respect to illegal telephone connection, using existing basic facilities and remotely load telephone subscription data.

CONSTITUTION: A controlling means UTF searches all of telephone subscription data regarding an isolated station SP and data, that shows the orders of remote loading based on a call request LID from the station SP. A coding means CDF encodes a secret data PIN. A processing means sends open data and secret data to an independent station. The independent station decodes the secret data and stores it in a memory.



LEGAL STATUS

[Date of request for examination]

02.10.1995

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

2685661

[Date of registration]

15.08.1997

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

.decision of rejection]

[Date of extinction of right]

(19)日本国特許庁(JP)

(12) 公開特許公報(A)

(11)特許出願公開番号

特開平6-237484

(43)公開日 平成6年(1994)8月23日

(51)Int.Cl.⁵

H 0 4 Q 7/04

識別記号

庁内整理番号

F I

技術表示箇所

C 7304-5K

審査請求 未請求 請求項の数19 O L (全 15 頁)

(21)出願番号 特願平3-126287

(22)出願日 平成3年(1991)5月29日

(31)優先権主張番号 9 0 0 6 6 6 2

(32)優先日 1990年5月29日

(33)優先権主張国 フランス(FR)

(71)出願人 591044452

フランス テレコム

FRANCE TELECOM

フランス国, 92131 イシレムーリノー

ル デュ ジェネラル レックラーク38-
40番地

(72)発明者 フランク・ラングラン

フランス国、エフ-75013 パリ、リュ・
ビュオ、19

(72)発明者 ジェラルド・マジョット

フランス国、エフ-75014 パリ、リュ・
デュ・ムラン・ペール、56

(74)代理人 弁理士 筒井 大和 (外1名)

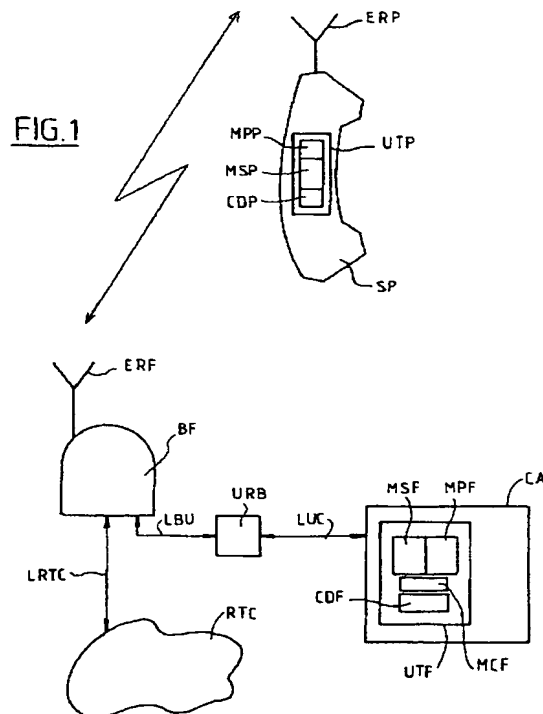
最終頁に続く

(54)【発明の名称】 独立局の電話加入データの遠隔ローディングのための電話装置

(57)【要約】

【目的】 不正電話接続に対する安全性の高い、また、現在の基礎施設を用いることのできる電話加入データの遠隔ローディングのための装置と方法の提供。

【構成】 独立局(SP)からの呼び出し要求(LID)に応じて、制御手段(UTF)が独立局(SP)に関するすべての電話加入データおよび遠隔ローディングの順序を示すデータをサーチする。コード手段(CDF)は秘密データ(PIN)をコード化する。処理手段は独立局に公開データおよび秘密データを送信する。独立局は秘密データをデコードし、メモリーに格納する。



【特許請求の範囲】

【請求項1】 ー 交換電話ネットワーク(RTC)に接続された少なくとも1つの固定ターミナル;

ー 少なくとも1つの独立局(SP)で、該独立局からの呼び出し要求の後に前記固定ターミナル(BF)と遠隔相互通信可能な少なくとも1つの独立局;該独立局は次の処理手段(UTP)を有する、すなわち:

・ 前記独立局(SP)に関する電話加入データを格納することを意図したメモリー(MPP、MSP)、および、

・ データをコード化/デコードする手段;

ー 前記固定ターミナルに接続され、前記電話加入データを電話接続を妨げる目的で制御することができる処理手段を設けた、認証手段(CA)、を有する電話装置であって、

前記認証手段の前記処理手段は:

ー 前記独立局に関する電話加入データおよび該電話加入データが該独立局に遠隔的にロードされなければならないことを示すことのできるデータを保持することのできるメモリー(MPF、MSF)、

ー 前記独立局のため少なくとも1つの特別キーを選択できる手段を備えた、変数キーデータのコード/デコード手段(CDF);

ー 要求により、前記独立局を特定することにより電話加入データをサーチすることのできる制御手段(MCF)、を有し、

前記認証手段(CA)の側においては、

・ 前記独立局(SP)から到来する、呼び出し要求のための公開数値ワード(LID)と該独立局を特定するための公開数値ワード(PID)に応じて、また、電話加入データの遠隔ローディングに関する所定の条件を確認するロード要求信号の存在のもとで、制御手段(UTF)が該独立局(SP)に関しすべての電話加入データおよび遠隔ローディングの順序を示すデータをサーチし、

・ 前記コード/デコード手段(CDF)が前記特別キー(EPID)すなわち秘密特別キー(PIN)を用いてコード化し、

・ 前記遠隔ローディングの順序を示すデータの値に応じて、処理手段(UTF)がコード化されない公開電話加入データおよび前記コード化された秘密電話加入データを前記独立局(SP)に送信し、

他方、前記独立局(SP)の側では、

・ コード/デコード手段(CDP)は、受け取った前記コード化された秘密電話加入データを特別キー(EPID)を用いて解読し、そして

・ 処理手段(UTP)は送信された秘密でない前記電話加入データおよび解読された秘密電話加入データを前記独立局のメモリーに格納する、ことを特徴とする電話装置。

【請求項2】 前記ロード要求信号が前記独立局からの信号であることを特徴とする請求項1の装置。

【請求項3】 前記独立局からの前記ロード要求信号が、前記呼び出し要求のための公開数値ワード(LID)を該独立局(SP)のキーボードに入力することからなることを特徴とする請求項2記載の装置。

【請求項4】 前記ロード要求信号が前記認証手段からの信号であることを特徴とする請求項1の装置。

【請求項5】 秘密でない前記公開電話加入データおよびコード化された前記秘密データの送信に引き続いて、前記認証手段の前記処理手段が認証要求のための公開数値ワード(AUTH_REQ)をランダムキーワード(RAND)と共に前記独立局に引き渡し;該認証要求のための公開数値ワード(AUTH_REQ)に応じて、前記独立局の前記コード/デコード手段(CDP)が、受け取った前記ランダムキーワードを遠隔ロードされた前記秘密電話加入データ(PIN)を用いてコード化し、該独立局のための付加的な特別キーを生成し、前記独立局が前記コード化されたランダムキーワード

(CPIN)を認証応答のための数値ワード(AUTH_RES)と共に前記認証手段に送信し、該認証応答のための数値ワード(AUTH_RES)に応じて、前記認証手段(CA)の前記コード/デコード手段(CDF)が前記コード化されたランダムキーワード(CPIN)を解読し、このようにデコードされた該ランダムキーワードを生成された前記ランダムキーワードと比較し、比較結果に応じて、電話加入データがロードされることを示すデータを前記独立局に格納し、電話接続を生成する、ことを特徴とする請求項1ないし4のいずれか1項の装置。

【請求項6】 前記秘密電話加入データが前記独立局の個人特定番号(PIN)であることを特徴とする請求項1ないし5のいずれか1項の装置。

【請求項7】 前記公開電話加入データが、前記呼び出し要求のための公開数値ワード(LID)、オペレータ特定のための数値ワード(OPSID)、前記独立局のサービスクラスに関する数値ワード(TCOS)、そして加入のための数値データ(TRD)からなることを特徴とする請求項1ないし6のいずれか1項の装置。

【請求項8】 前記コード/デコード手段が前記独立局の前記個人特定番号(PIN)を変数データ(EPIN1、EPIN2)、および暗号関数Fによる前記特別キー(EPID)を用いた該変数データ(EPIN1、EPIN2)の変換(S1、S2)に応じてコード化/デコードすることを特徴とする請求項6の装置。

【請求項9】 前記コード/デコード手段が前記独立局の前記個人特定番号(PIN)を、変数データ(EPIN1、EPIN2)および、該変数データの暗号関数Fによる、特別キー(EPID)および付加的な変数データ(EPIN3)を用いた変換(S1、S2)に応じてコ

ード化／デコードすることを特徴とする請求項6の装置。

【請求項10】 前記独立局が、補助的認証手段(CAA)がデータの交換を目的として前記認証手段(CA)と接続された、補助的交換電話ネットワークと遠隔相互通信ができ、該補助的認証手段の処理手段(UTFA)が：

ー 前記独立局に関する仮電話加入データを保持することのできるメモリー(MPFA、MSFA)；
ー 前記独立局のための該仮電話加入データを生成することが
10 できる制御手段(MCFA)；を有し、そして、前記認証手段(CA)の側では、

・ 前記補助的電話ネットワーク(CAA)との接続要求のための公開数値ワード(ROAMING)に応じ、該接続要求のための公開数値ワード(ROAMING)が認証手段による前記独立局の認証に関する所定の条件を確認する時、前記処理手段が変数データ(EPIN1、EPIN2)を生成し、秘密電話加入データにより形成された特別キー(PIN)を用いて該変数データの変換(S1、S2)を計算し、

・ 前記処理手段(UTF)が前記変数データ(EPIN1、EPIN2)および計算された該変数データの変換(S1、S2)を前記補助的認証手段(CAA)に送信し；

前記補助的認証手段の側では、

・ 前記制御手段(MCFA)が仮公開電話加入データを生成し；

・ 前記制御手段が仮秘密電話加入データ(RPIN)を生成し、受け取った前記変数データ(EPIN1、EPIN2)および該変数データの前記変換(S1、S2)を用いて該仮秘密電話加入データをコード化し、

・ 処理手段(UTFA)がコード化された前記仮秘密電話加入データを生成された前記公開仮電話加入データと共に前記独立局へ送信し、

前記独立局(SP)の側では、

・ 前記コード／デコード手段(CDP)が、受け取ったコード化された前記仮秘密電話加入データを、前記秘密電話加入データにより生成された前記特別キー(PIN)を用いて解読し、そして、

・ 前記処理手段(UTF)が、受け取った秘密でない前記公開仮電話加入データおよびコード化された前記秘密データを前記メモリー(MPP、MSP)に格納する、ことを特徴とする請求項1ないし9のいずれか1項の装置。

【請求項11】 前記仮秘密電話加入データが前記独立局の前記個人特定番号(RPIN)からなることを特徴とする請求項10の装置。

【請求項12】 前記公開電話加入データが、前記呼び出し要求のための公開数値ワード(LID)、前記オペレータの特定のた

独立局のサービスクラスに関する数値ワード(TCOS)、そして前記加入の数値データ(TRD)からなることを特徴とする請求項10および11のいずれか1項の装置。

【請求項13】 前記コード／デコード手段が前記独立局の前記仮個人特定番号(RPIN)を前記変数データ(EPIN1、EPIN2)、および前記特別キー(PIN)を用いた暗号関数Fによる該変数データの前記変換(S1、S2)に応じてコード化／デコードすることを特徴とする請求項11の装置。

【請求項14】 前記コード／デコード手段が、前記独立局の前記仮個人特定番号(RPIN)を、前記変数データ(EPIN1、EPIN2)、および前記特別キー(PIN)ならびに前記補助的認証手段の制御手段により生成された付加的な変数データ(EPIN3)を用いた暗号関数Fによる該変数データの前記変換(S1、S2)に応じてコード化／デコードすることを特徴とする請求項11の装置。

【請求項15】 前記認証手段(CA)あるいは前記補助的認証手段(CAA)が、すべての前記独立局および前記交換ネットワーク(RTC)あるいは前記補助的交換ネットワーク(STCA)のすべての前記固定ターミナルのための一般認証センターと通じることを特徴とする請求項1ないし14のいずれか1項の装置。

【請求項16】 前記認証手段(CA)あるいは前記補助的認証手段(CAA)が固定ターミナルに収容され、前記独立局のすべて、および前記交換ネットワーク(RTC)あるいは前記補助的交換ネットワーク(RTCA)の前記固定ターミナルのすべてのための一般認証センターと接続されていることを特徴とする請求項1ないし14のいずれか1項の装置。

【請求項17】 請求項1ないし9、15、16のいずれか1項の電話装置に利用されることを目的とする、電話加入データの遠隔ローディングの方法であって、認証手段(CA)の処理手段には：

ー 独立局に関する電話加入データおよび該電話加入データが該独立局に遠隔ローディングされなければならないことを示すことのできるデータを通信により保持することができるメモリー(MPF、MSF)；

ー 前記独立局のための少なくとも1つの特定キーを選択できる手段を備えた、変数キーデータのコード／デコード手段(CDF)；

ー 要求により、前記独立局を特定することにより前記電話加入データをサーチすることができる制御手段(MCF)；が設けられ、

次のステージ、すなわち：

a) 前記認証手段(CA)の側において、

・ a1) 前記独立局(SP)からの呼び出し要求のための公開数値ワード(LID)と該独立局の特定のた

ータ遠隔ローディングに関する所定の条件を確認する要求信号の存在のもとで、該独立局（SP）に関するすべての前記電話加入データおよび遠隔ローディングの順序を示すデータをサーチし、

- ・ a 2) 特別キー（EPID）を用いて秘密データ（PIN）をコード化し、
- ・ a 3) 遠隔ローディングの順序を示すデータの値に応じて、秘密でない公開加入データおよびコード化された前記秘密データを前記独立局（SP）に送信し、
- b) 前記独立局（SP）の側において、
 - ・ b 1) 受け取ったコード化された秘密電話加入データを特別キー（EPID）を用いてデコードし、
 - ・ b 2) 送信された秘密でない前記公開電話加入データおよびデコードされた前記秘密電話加入データを前記独立局（SP）の前記メモリに格納する、からなる、ことを特徴とする電話加入データの遠隔ローディング方法。

【請求項18】 請求項10ないし16のいずれか1項の電話装置に利用されることを目的とする、電話加入データの遠隔ローディングの方法であって、前記独立局は、補助的認証手段（CAA）がデータ交換ができるため認証手段（CA）に接続された補助的交換電話ネットワークと遠隔相互通信でき、該補助的認証手段（CAA）の処理手段（UTFA）には：

- ー 前記独立局に関する仮電話加入データを保持できるメモリ（MPFA、PSFA）；
- ー 前記独立局のための仮公開電話加入データを生成することができる制御手段（MCFA）；が設けられ、次のステージ、すなわち：

- 1) 前記認証手段（CA）の側においては、
 - ・ 1 1) 前記補助的認証手段（CAA）から前記補助的電話ネットワークへの接続要求のための公開数値ワード（ROAMING）に応じて、該接続要求のための公開数値ワード（ROAMING）が前記認証手段による独立局の認証に関する所定の条件を確認する時、変数データ（EPIN1、EPIN2）を生成し、秘密電話加入データにより生成された特別キー（PIN）を用いて該変数データの変換（S1、S2）を計算し、
 - ・ 1 2) 前記変数データ（EPIN1、EPIN2）および計算された該変数データの前記変換を補助的認証センター（CAA）に送信し、
- 2) 前記補助的認証手段の側においては、
 - ・ 2 1) 前記仮公開電話加入データを生成し、
 - ・ 2 2) 仮秘密電話加入データ（RPIN）を生成し、前記変数データ（EPIN1、EPIN2）および該変数データの前記変換（S1、S2）を用いて該仮秘密電話加入データをコード化し、
 - ・ 2 3) コード化された前記仮秘密電話加入データを、生成された前記仮公開電話加入データと共に前記独立局

に送信し、

- 3) 前記独立局（SP）の側では、

- ・ 3 1) 受け取ったコード化された前記仮秘密電話加入データを、前記秘密電話加入データにより生成された前記特別キー（PIN）を用いて解読し、そして、
- ・ 3 2) 受け取った秘密でない前記仮公開電話加入データおよびデコードされた秘密データを前記メモリ（MPFA、MSPA）に格納すること、からなる、ことを特徴とする電話加入データの遠隔ローディング方法。

10 【請求項19】 ステージ22が付加的な次のステージ、すなわち：

- * 2 2 1) 付加的な変数データ（EPIN3）を生成し、補足的な該変数データ（EPIN3）をさらに用いて前記電話加入データをコード化する、ステージをさらに含むことを特徴とする請求項18の方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、独立局の電話加入データの遠隔ローディングに関する。本発明は、GSM（特別移動グループ、Group Special Mobile）、DCT（デジタルコードレス電話、Digital Cordless Telephone）と呼ばれるシステムおよび無線インタフェースCAI（共通無線インタフェース、Common Air Interface）のような、移動あるいは固定独立局を有する電話通信システム、特にフランスのポアンテル（POINTEL、登録商標）システムにおいて実施することができる。

【0002】

【従来の技術】一般的に言って、そのような通信システムは、交換電話ネットワークに接続された少なくとも1つの固定ターミナル、および、自分からの呼び出し要求の後にその固定ターミナルと遠隔相互通信が可能少なくとも1つの独立局を有している。

【0003】非常にしばしば、独立局の特定はその独立局の電話加入データにより決定される。

【0004】電話接続の要求が独立局から送信される時はいつでも、電話加入データに応じて電話接続の生成を妨げることでできる、交換ネットワークに接続された認証センターにより、独立局からの電話加入データが統制されている。

40 【0005】実際的には、不正電話接続の発生を避けるため、電話加入データの少なくとも1部は秘密あるいは機密要素を有している。

【0006】NMT（北欧移動電話、Nordic Mobile Telephone）やRADIO COM2000と呼ばれるシステムのような第一世代の移動独立局を有する電話通信システムにおいては、電話設備の取付者あるいはセールスマンにより電話加入データが移動独立局にロードされた。

【0007】

50 【発明が解決しようとする課題】このローディング方法

は次のような問題を有する。すなわち、商業的な供給における適応性と融通性の不十分さ、電話設備のセールスマンとサービス提供者の役割の混同、そして、不正接続に対する低レベルの安全防護、である。

【0008】GSMのような第二世代の移動独立局を有する電話通信システムにおいては、着脱可能な加入モジュールに電話加入データがプログラムされていることを考えている。この解決は前記のローディング方法により多くの安全性を付与するという点で優れている。それにもかかわらず、着脱可能な加入モジュールに加入データをプログラムすることは特別の設備によってなされるので、電話加入権の分配のために大きな基礎施設が必要である。

【0009】本発明はこの問題を解決することを本質的な目的としている。

【0010】

【課題を解決するための手段】このように、本発明の1つの目的は、独立局からの電話加入データの遠隔ローディングの方法を提供することである。

【0011】本発明は、次のものを有する電話装置に関するものである。すなわち：

- 交換電話ネットワークに接続された少なくとも1つの固定ターミナル；
- 自分からの呼び出し要求の後に固定局と遠隔相互通信の可能な少なくとも1つの独立局であって、次の処理手段を有する独立局；
 - ・ その独立局に関する電話加入データを格納できるメモリー、そして、
 - ・ コード／デコード手段；
- 固定局に接続され、電話接続の開始を妨げるため電話加入データを制御することのできる処理手段を備えた認証手段。

【0012】本発明の一般的な定義によれば、認証手段の処理手段は次のものを有している；すなわち、

- 独立局に関する電話加入データ、およびその電話加入データが前記独立局に遠隔ローディングされるべきことを示すことのできるデータを格納することができるメモリー；
- 独立局のための少なくとも1つの特別キーの選択を可能にする手段と共に、変数キーデータをコード／デコードするための手段；
- 要求に応じて、独立局を特定することにより電話加入データをサーチすることのできる制御手段；そして認証手段のレベルにおいては、
 - ・ 独立局の特定の公開数値ワードと共に独立局から発信される呼び出し要求の公開数値ワードに応じて、そして電話加入データの遠隔ローディングに関する所定の条件を実証するロード要求信号の存在のもとで、制御手段は独立局に関するすべての電話加入データを、遠隔ローディングの順序に関するデータと共にサーチし、

・ コード／デコード手段は特別キーを用いて秘密データをコード化し、

・ 処理手段は秘密ではない公開電話加入データをこのようにコード化された秘密データと共に、遠隔ローディングの順序を示すデータの値に応じて、独立局に送信することを許可し、独立局のレベルにおいては、

・ コード／デコード手段は受け取ったコード化された秘密電話加入データを特別キーの助けにより解読し、

・ 処理手段は、コード化されずに送信された秘密ではない公開電話加入データとデコードされた秘密データを独立局のメモリーに格納する。

【0013】このような装置は、電話加入データのプログラムあるいは遠隔ローディングのための特別の設備を必要とせず、現存の通信ネットワークの基礎施設を電話加入権の分配や管理のために使用することができる。

【0014】さらに、秘密電話加入データをコード化して送信することにより、この電話加入データの遠隔ローディングの安全性を非常に高いものにする。

【0015】本発明の好ましい実施例によれば、ロード要求信号は独立局から発信される信号である。

【0016】実際的には、独立局から発信される要求信号は、呼び出し要求のための公開数値ワードを独立局のキーボードに入力することからなっている。

【0017】本発明の他の実施例によれば、ロード要求信号は認証手段から発信される信号である。

【0018】本発明の他の側面によれば、秘密ではない公開電話加入データのコード化されない送信ならびにコード化された秘密データの送信の後に、認証に関する処理手段は独立局に対し認証要求のための公開数値ワードと欄ダムキーワードを送信し、認証要求のための数値ワードに応じて、独立局のコード／デコード手段はこのように受け取ったランダムキーワードを、遠隔ロードされた秘密電話加入データを用いてコード化し、この独立局に特定のもう1つのキーを作り出し、独立局はこのコード化されたランダムキーワードを認証手段に、認証応答のための数値ワードと共に、送信し、そして、この認証応答のための数値ワードに回答して、認証手段のコード／デコード手段はこのように受け取ったコード化されたランダムキーワードをデコードし、デコードされたランダムキーワードを生成されたランダムキーワードと比較し、この比較に応じて、電話加入データが独立局にロードされていることを示すデータを格納し、電話接続を実現する。

【0019】実際的には、秘密電話加入データは独立局の個人特定番号からなっている。

【0020】実際的には、公開電話加入データは呼び出し要求のための公開数値ワード、オペレータの数値識別ワード、独立局のサービスクラスに関する数値ワードおよび数値加入データを含むものである。

【0021】本発明の他の側面によれば、コード／デコ

ード手段は、変数データおよび暗号関数Fによるその変換に応じ、特別キーと付加的な変数データの助けを得て独立局の個人特定番号をコード化／デコードする。

【0022】本発明の1変形によれば、独立局は補助的交換電話ネットワークと遠隔相互通信が可能であり、その補助的交換電話ネットワークの補助的認証手段は認証手段と互いの間でデータの交換ができるように接続されており、補助的認証手段の処理手段が、次のものを有していることを特徴とする、すなわち、

ー 独立局に関する仮電話加入データを格納することができるメモリ；

ー 独立局のための仮電話加入データを生成することができる制御手段；そして、認証手段のレベルでは、

・ 補助的認証手段から発信される補助的電話ネットワークとの接続要求のための公開数値ワードに応じて、接続要求のための公開数値ワードが認証手段による独立局の認証に関する所定の条件を実証するとき、処理手段は変数データを生成し、秘密電話加入データから形成された特別キーの助けによりその変換を計算し、

・ 処理手段は変数データおよびこのように計算されたその変換を補助的認証手段に送信し；補助的認証手段のレベルでは、

・ 制御手段が仮公開電話加入データを生成し、
・ 制御手段は仮秘密電話加入データを生成し、それを受け取った変数およびその変換によりコード化し、

・ 処理手段はこのようにコード化された仮秘密電話加入データを生成された仮公開電話加入データと共に独立局に送信し、独立局のレベルでは、

・ コード／デコード手段が、受け取ったコード化された秘密電話加入データを、秘密電話加入データにより形成された特別キーの助けにより解読し、処理手段はコード化されないで受け取った秘密でない仮公開電話加入データ、およびデコードされた秘密データをメモリに格納する。

【0023】このような装置は、先に認証手段と補助的認証手段の間で秘密電話加入データを送信することなく補助的認証手段のレベルで秘密電話加入データを生成することができ、また、それにより仮電話加入データの遠隔ローディングの安全性が高まるという点で有利である。

【0024】仮秘密電話加入データを独立局の仮個人特定番号とするのが实际的である。

【0025】実際的には、仮公開電話加入データは、呼び出し要求のための公開数値ワード、オペレータの数値特定ワード、独立局のサービスクラスに関する数値ワード、そして数値加入データからなるものとしてすることができる。

【0026】本発明の他の側面によれば、コード／デコード手段は、独立局の仮個人特定番号を変数データ、ならびに特別キーを用いたその変数データの暗号関数Fに

よる変換に応じてコード化／デコードする。

【0027】コード／デコード手段が独立局の仮個人特定番号を、変数データ、特別キーを用いた暗号関数Fによるその変換、および補助的認証手段の制御手段により生成された付加的な変数データに応じてコード／デコードするのは有利である。

【0028】本発明の他の特徴によれば、認証手段あるいは補助的認証手段が、すべての独立局ならびに交換ネットワークあるいは補助的交換ネットワークのすべての固定ターミナルのために機能する一般認証センターと通じるものである。

【0029】本発明の他の特徴によれば、認証手段あるいは補助的認証手段は固定ターミナルに収納され、すべての独立局ならびに交換ネットワークの固定ターミナルのための一般認証センターに接続されている。

【0030】本発明は、電話装置で用いられることを意図した電話加入データの遠隔ローディング方法を含むものである。

【0031】本発明の方法によれば認証手段の処理手段には次のもの、すなわち：

ー 独立局に関する電話加入データおよびその電話加入データがその独立局に遠隔ロードされなければならないことを示すことができるデータを、通信により、格納できるメモリ；

ー 独立局のための少なくとも1つの特別キーの選択を可能にする手段を備えた、変数キーデータをコード／デコードするための手段；

ー 要求に応じ、独立局を特定することにより電話加入データをサーチすることができる制御手段、を設けることが提案され、この方法は次のステップ、すなわち：

a) 認証手段のレベルにおいて、

・ a1) 独立局からの公開特定数値ワードと共に、また、制御信号の存在のもとで、独立局から発信される呼び出し要求のための公開数値ワードに応じて、電話加入データの遠隔ローディングに関する所定の条件を検証し、独立局に関するすべての電話加入データならびに遠隔ローディングの順序を示すデータをサーチし、

・ a2) 秘密の特別キーデータの助けを得てコーディングし、

・ a3) 遠距離ローディングを示すデータの値に対応して、秘密ではない公開の電話加入データをコード化しないまま、そして秘密データはコード化して前記独立局に送信することを許可し、

b) 独立局のレベルにおいて、

・ b1) 受け取った秘密電話加入データを特別キーを用いてデコードし、

・ b2) 送信された秘密でない公開加入データ、ならびにデコードされた秘密データを独立局のメモリに格納する、ことからなるものである。

【0032】本発明の特に興味深い変形として、本発明

の電話加入データの遠隔ローディング方法は、補助的認証手段が認証手段との間でデータの交換を可能にする目的でその認証手段と接続されている補助的交換電話ネットワークと独立局が遠隔相互通信できる電話装置にも適用することができる。

【0033】この変形方法においては、補助認証手段の処理手段は次のもの、すなわち：

— 独立局に関する仮電話加入データを格納することができるメモリー；

— 独立局のための仮電話加入データを生成することができる制御手段；を備えており、そして、この方法が次のステップ、すなわち：

1) 認証手段のレベルにおいて、

・ 11) 補助的認証手段から発信される補助的電話ネットワークとの接続要求のための公開数値ワードに応じて、接続要求のための公開数値ワードが独立局の認証に関する認証手段による所定の条件を証明した場合、変数データを生成し、秘密電話加入データにより形成される特別キーを用いてその変換を計算し、

・ 12) 変数データならびに前記のように計算されたその変換を補助認証手段に送信し、

2) 補助認証手段のレベルでは、

・ 21) 仮公開電話加入データを生成し、

・ 22) 仮秘密電話加入データを生成し、変数データならびにその変換を用いてその仮秘密電話加入データをコード化し、

・ 23) このようにコード化された仮電話加入データを、生成された公開仮電話加入データと共に、独立局に送信し、

3) 独立局のレベルでは、

・ 31) 受け取られたコード化された秘密電話加入データを秘密電話加入データを用いてデコードし、そして、

・ 32) 受けとられたコード化されていない仮公開電話加入データおよびデコードされた秘密データをメモリーに格納する、ことからなるもの考えることができる。

【0034】ステージ22がさらに次のステップ、すなわち：

* 221) 付加的な変数データを生成し、電話加入データをさらにこの補足的な変数データを用いてコード化する、ことからなるものとするのは有利である。

【0035】本発明の他の特徴および有利な点は以下の詳細な説明とそれに関連する図面からより一層明らかになるであろう。

【0036】

【実施例】図1はアングロサクソンの規格であるCAI（共通無線インタフェース、Common Air Interface）のMPT1375規格に基づくポアンテル（POINTEL、登録商標）タイプの遠距離通信ネットワークに用いられることを意図した電話装置を示す線図である。

【0037】移動可能なあるいは固定の独立局SPは、

独立局SPからの呼び出し要求を経て、固定ターミナルBFと遠隔遠距離通信を行なうことができる。独立局SPは送受信機およびアンテナを有する組立体ERPを備えている。

【0038】固定ターミナルBFの側には、固定ターミナルと独立局間の遠隔相互通信のための送受信機およびアンテナを有する組立体ERFが設けられている。

【0039】CAI規格の規定によれば、独立局と固定ターミナル間の無線伝送手段は、電話チャンネル（B）および数値信号チャンネルDから構成されている。

【0040】固定ターミナルは交換電話ネットワークLRTCに接続されている。CAI規格の規定によれば、独立局は：

— 独立局からの公開電話加入データを格納するための公開メモリー領域MPPと、その独立局からの秘密電話加入データを格納するための秘密メモリー領域MSPとに分割されたメモリー、および、

— データのコード/デコード手段CDP、を有する処理手段UTPを備えている。

【0041】独立局のメモリーをプロテクトされた領域とプロテクトされていない領域に分割することは安全性を高めるために有益であることに注目できる。しかし、この分割は本発明の実施のために必須ではない。

【0042】最後に、本装置にはターミナル接続ユニットURBを介して固定ターミナルに接続された認証手段CAが設けられている。特定電話接続LBUにより、ターミナル接続ユニットURBと固定ターミナルBFとの結合が可能とされており、他方、数値信号線（LUC）により認証手段CAとターミナル接続ユニットURBとの結合が可能とされている。

【0043】認証手段CAは、独立局からの電話加入データを保持し、固定ターミナルと独立局の間の電話接続の成立を阻止するため電話加入データを制御できるメモリーを備えた処理手段UTFからなっている。認証手段のメモリーが、独立局からの公開電話加入データを格納できる公開メモリー領域、およびその独立局の秘密電話加入データを格納できる秘密メモリー領域MSFに分割するのは有利である。

【0044】勿論、この分割は本発明の実施に必須のものではない。

【0045】ここで、認証手段CAはすべての独立局および交換ネットワークRTCの固定ターミナルのための一般認証センターに対応することができることに注目すべきである。

【0046】また、認証手段が少なくとも1つの固定ターミナルに収納され、それがすべての独立局および交換ネットワークRTCの固定ターミナルのための一般認証センターに接続されている、独立局を有する遠隔通信システムが存在し得ることに注目できる。

【0047】以下の説明において、認証手段が交換ネッ

トワークの認証センターに対応する通信システムだけが考慮される。しかし、本発明のこの本質的な要素手段は固定ターミナルに収容される認証手段にも適用することができる。

【0048】ポアンテル (POINTEL、登録商標) からの電話加入データは加入契約の際にポアンテルの契約担当者から加入者に割り当てられる。このデータは独立局がポアンテル・サービスにアクセスするのを認められるのに必要である。

【0049】CAI規格によれば、電話加入データは次のものを含んでいる、すなわち：

- 無線接続を確立するため固定ターミナルに送られる最初のバケットのビットに対応する、呼び出し要求のための公開数値ワードLID (リンク特定データ、Link Identification Data)、このサイズは16ビットである；
- 独立局の秘密特定番号に関する数値ワードPIN (個人特定データ、Personal Identification Number)、このサイズは64ビットである；
- オペレーションの特定の目的のための数値ワードOPSI C (オペレータ特定コード、Operators Identity Code)、このサイズは9ビットである；
- 独立局のサービスのクラスに関する数値ワードTCOS (サービスの通信クラス、Telecom Class of Service)、サイズは3ビット；そして、
- それだけで独立局の加入を特定する目的のための付加的電話加入データに関する数値データTRD (通信ポイント登録データ、Telepoint Registration Data)、サイズは最大80ビット。

【0050】CAI規格によれば、無線電話接続を実現するために、数値ワードLID、PIN、OPSI CおよびTCOSが必須である。CAI規格はこれらのワードのサイズも規定している。他方、ワードTRDについてはオペレータの裁量に委ねられている。例えば10進コードとしてもよい。

【0051】他方、ワードOPSI Cは加入が承認されたポアンテル契約者を特定するものである。

【0052】一般的に言って、電話加入データは、それが割り当てられた後、ポアンテル呼び出しの際、要求されたサービスを提供する前に、独立局を認証するために用いられる。

【0053】当面、CAI規格は、電話設備の取付者あるいはセールスマンによる、独立局の電話加入データのマニュアルローディングを規定している。

【0054】今では、そのような電話加入データのローディング方法は、電話設備のセールスマンあるいは加入者からのマニュアルな介入が必要であり、不正な加入に対する安全性が低いという点で、不満足なものである。

【0055】出願人は、ポアンテル型の電話装置の基礎構造を修正すること無しに、上記の問題点を解決するこ

とのできる、電話加入データの遠隔ローディング方法を提供するという問題に直面した。

【0056】図2および図3は本発明による電話加入データの遠隔ローディングのプロトコルの必須な要素段階を線図により示したものである。

【0057】遠隔ローディングのプロトコルは、独立局から発せられる呼び出し要求に関するE1ステージにより開始される。

【0058】E1ステージは、固定ターミナルBFとの無線接続を確立することを目的として独立局において受話器をフックから外すことにより開始される。アクセスはランダムであり、CAI規格により割り当てられる40のチャンネルのうちの1つを介して達成される。無線接続は、呼び出し要求のための公開数値ワードLIDが交換された電話ネットワークにより受理された時に、固定ターミナルBFとの無線接続が確立される。

【0059】ステージE2において、独立局は固定局との間で互いに補足し合うメッセージを交換し、これにより独立局を認証できる。

【0060】より具体的に言えば、独立局は独立局の能力に関するメッセージTERM_CAP (ターミナル能力情報要素、Terminal Capabilities Information Element) と独立局の活動に関するメッセージFA3, n (特徴活動情報要素、Feature Activation Information Element) を発する。メッセージTERM_CAPおよびFA3, nにより独立局は固定ターミナルに対し自分自身を表示することができる。

【0061】メッセージTERM_CAPおよびFA3, nに応じて、固定ターミナルは、独立局のスクリーンを消去する命令に関するメッセージDISP=FF、およびその後 (ステージE23およびE24において) 認証されるという条件で、(この場合メッセージFA3, nにより) 要求されたサービスを受理するメッセージF13, nを送る。

【0062】そのほかに、固定ターミナルBFは、固定ターミナルにより認証された、独立局の電話能力に関するメッセージBAS_CAP (基底能力情報要素、Base Capabilities Information Element) を発する。

【0063】E23ステージの時に、固定ターミナルはランダムなキーワードRANDを生成し、このランダムキーワードRANDを認証要求に関する公開数値ワードAUTH_REQと共に独立局に発信する。

【0064】認証要求のための数値ワードAUTH_REQに応じて、独立局のコード/デコード手段CDPは受け取ったランダムキーワードRANDを独立局用の特別なキーの助けを得てコード化する。例えば、特別なキーはその独立局の秘密電話加入データ、特にその個人特定番号PIN、により作成することができる。

【0065】次に、独立局はこのようにコード化されたランダムキーワードCPINを認証の応答のための公開

数値ワードAUTH_RESと共に固定ターミナルBFに送る。独立局は、独立局のメモリーに秘密電話加入データPINが無い結果、ランダムワードのコード化が無効である場合、認証されないと考えられる。

【0066】他方、秘密電話加入データPINが独立局のメモリーにある場合、独立局の認証に関するステージE2は肯定的なものとなり、認められた電話接続が生成される結果となる。

【0067】更に詳しく説明すると、認証の応答のための数値ワードAUTH_RESに応答して、認証センターのコード／デコード手段CDFは受け取ったランダムキーワードコードCPINを、特別のキーPINの助けを得て解読し、このようにデコードしたランダムキーワードを固定ターミナルにより生成されたランダムキーワードと比較し、その比較結果に基づいて電話接続の生成を認める。

【0068】ステージE3は独立局のキーボードからの呼び出し番号の列挙からなっている。

【0069】ここで、これら3つのステージE1ないしE3は現行のCAI規格にすでに存在しているものであることに注目できる。

【0070】本発明によれば、ステージE3に引き続いて、ステージE4が考慮されるが、それは次のように展開する。

【0071】まず第1に、認証センターは固定ターミナルから、第1の呼び出しを行ないたいと希望している、独立局の特定情報を受け取る。この特定情報はワードPID、TCOS、OPSIC、TRDおよびLIDからなるメッセージを送ることが含まれている。次いで、認証センターはワードLID、FA3、nにより、そして電話呼び出しの場合は希望の電話番号により、求められているサービスを決定する(ステージ41)。

【0072】呼び出し要求のための数値ワードLIDに応じて認証センターは独立局から発せられている呼び出し要求に答えるべきかどうか決定する。

【0073】非常に有利なことに、本発明によれば、LIDが電話加入データの遠隔ローディングの要求を伴った呼び出し要求に関する場合、それを見分けることができる。

【0074】例えば、電話加入データの遠距離ローディングを希望する場合、電話加入データの遠距離ローディングのための特別なLIDをキーボードに入力することが考えられる(LIDのマニュアル生成)。

【0075】ここで、CAI規格によればLIDは0から7まででなる4桁の数字であり、16進では0000から03EFまでである、ことに注目できる。

【0076】本発明によれば、さらに、電話加入データが独立局へ遠隔的にロードされるべきであることを示すデータは、認証センターの処理手段のメモリーに格納されるべきである、ことを考えることができる。

【0077】まず第1に、独立局から、独立局からの特定PIDと共に、電話加入データの遠隔ローディングに関する所定の条件を証明するロード要求信号の存在のもとに発せられる呼び出し要求LID(ここではLIDのマニュアル生成)に回答して、制御手段は、独立局に関する、また遠隔ローディングの順序を示す、すべての電話加入データにわたりサーチを行なう(ステージE43)。

【0078】次いで、コード／デコード手段CDFは秘密電話加入データを特別のキーの助けを得てコード化する(ステージE44)。

【0079】最後に、処理手段UTFは、秘密では無い公開電話加入データをコード化された秘密データと共に独立局SPに遠隔ローディングの順序を示すデータの値の関数として送信することを許可する(ステージE6)。

【0080】他方、呼び出し要求のための公開数値ワードLIDが自動的に生成される場合は、それは独立局が電話加入データを要求しないか、あるいは既に個人として特定されていることを意味する。

【0081】独立局からの認証の証明結果に応じて、認証センターの処理手段は電話接続の生成を許可するか、あるいは独立局からの呼び出し要求をさらに取り扱うことをしない(ステージE5)。

【0082】より詳しく言えば、認証証明の要求は次のように展開する。

【0083】認証要求のための数値ワードAUTH_RESに応じて、認証センターのコード／デコード手段CDFは受けとられたランダムキーワード、すなわちコード化されたCPIN、を特別キーPINの助けによりデコードし、このようにデコードしたランダムキーワードを生成されたランダムキーワードと比較し、比較の関数として、電話接続の生成を許可する。

【0084】遠隔ローディングの順序を表すデータの値により独立局が遠隔的にロードされるべきであることが示される時、ステージE6がその役割を果たす。

【0085】電話加入データの発信は2つの部分、すなわち1つは公開電話加入データに関する部分、そしてもう1つは秘密電話加入データに関する部分に分けることは非常に有利である。

【0086】ステージE61の時、数値ワードTRD_ALLLOCの発信により電話加入データTRDの発信が可能である。

【0087】秘密電話加入データの方は、数値ワードPIN_ALLLOCにより発信される。

【0088】本発明によれば、秘密電話加入データはその秘密データが不正に横取りされることを避けるためコード化されて発信される。

【0089】本発明によれば、秘密電話加入データのローディングは、その独立局のための特別キーの選択が可能

能な手段と共に、認証センターのデータコード／デコード手段により達成される。

【0090】次に図4が参照される。

【0091】ここで、秘密電話加入データのコーディングに用いられる特別キーはキーE P I D（暗号化された携帯特定データ、Encrypted Portable Identification Data）である。

【0092】勿論、この独立局のための特別キーE P I Dは、独立局S Pと認証センターC Aにおいて同時に格納されている。

【0093】実際的には、認証センターの制御手段が、それぞれ32ビットのサイズを有する第1および第2のランダム数E P I N 1およびE P I N 2を最初に生成する。

【0094】次いで、制御手段が、変換S 1と、変換S 2と 2^{32} の積との和の助けを得て（秘密加入データを表す）個人特定番号P I Nを生成し、それにより64ビットからなるP I Nを得ることができる。

【0095】場合によっては、制御手段は64ビットの値の補足の変数データE P I N 3の助けを更に得てP I Nを生成するが、このE P I N 3は、やはり制御手段により生成され、排他的論理和によって前記の計算を完成するものである。

【0096】このように、秘密電話加入データをコード化した仕方では遠隔ローディングするのを可能とするのは、変数ワードE P I N 1、E P I N 2そして（場合により）E P I N 3である。

【0097】これらのワードE P I N 1、E P I N 2そして（場合により）E P I N 3を受け取ると、独立局のコード／デコード手段はまず第1に暗号関数Fを用い、秘密キーE P I Dの助けを得てワードE P I N 1、E P I N 2のそれぞれの変換S 1とS 2を計算する。最後に、S 1、S 2そして（場合により）E P I N 3の助けにより秘密加入データP I Nを回復するための計算が行なわれる。

【0098】秘密ならびに公開電話加入データが独立局において正しく遠隔的にロードされたことを証明するために、先に説明したステージE 23と同じ、認証要求のためのステージE 81が提供される。言い替えれば、このステージは、認証要求のための数値ワードA U T H _ R E Qをランダム数R A N Dと共に独立局へ送ることを含むものである。

【0099】認証要求のための数値ワードA U T H _ R E Qに応じて、独立局のコード／デコード手段C D Pは受け取ったばかりのランダムキーワードR A N Dを、独立局に関する秘密加入データP I Nの助けによりコード化する。この秘密加入データP I Nは前にワードE P I N 1、E P I N 2そしてE P I N 3を中間形態としてコード化されて発信されたものであり、キーE P I Dを介してデコードされたものである。

【0100】次いで、独立局S Pは、このようにコード化されたランダムキーワードC P I Nを認証応答のための数値ワードA U T H _ R E Sと共に認証センターC Aに送る。この認証応答のための数値ワードA U T H _ R E Sに応じて、認証センターのコード／デコード手段は、このようにして受け取ったコード化されたランダムキーワードC P I Nを特別キーP I Nの助けを得てデコードする。最後に、認証センターはこのようにデコードされたランダムキーワードを生成されたランダムキーワードと比較し（ステージE 82）、比較結果に応じて電話接続を確立する（ステージE 9）。

【0101】実際的には、1つの1バイトの公開数値ワードU S Eをデータの性質を示すためのものとするのが考えられる。例えば、バイトの第1ビットをデータのコーディングに関するものとする（0はコード化されておらず、1はコード化されていることを示す）。バイトの第2ビットは加入の性質に関するものとする（0はメイン、1は補助、言い替えれば、後に詳しく説明されるR O A M I N Gサービスを示す）。他のビットは独立局のそれぞれのメモリーにデータを格納するため0に維持される。

【0102】独立局に公開数値ワードP I N _ A L L O Cの利用を示すのはワードU S Eであることに注目すべきである。

【0103】同様に、1つの1バイトの数値ワードA U T H _ N Oの利用を考えることができる。この機能はデータをコード／デコードするために独立局にその暗号関数のうちどれを用いるべきかを示すことにある。もし独立局が利用できる1つの暗号関数だけしか持っていないのであれば、ワードA U T H _ N Oの効果は無い。

【0104】先に説明した実施例においては、メッセージP I N _ A L L O CおよびT R D _ A L L O Cを介して公開ならびに秘密電話加入データのローディングの開始を可能とするのは、キーボードから入力され、独立局から出される呼び出し要求のためのワードL I Dである。

【0105】この例においては、受話器がフックから外される時、自動的に独立局により生成されるワードL I Dは、その電話加入データの遠隔ローディングを可能としない。

【0106】その結果、独立局の利用者が望む場合（つまり、ここでは、キーボードからL I Dが入力された場合）にだけ、電話加入データが遠隔送信される。

【0107】独立局（あるいはその加入者）がどんな制御にも影響を与えることなく、あるいはどんな特定のサービスを要求することなく、電話加入データの少なくとも一部を修正する場合などの特定の適用の場合のために、遠隔ローディング方法を開始させるロード要求信号は認証手段からのロード要求とすることができる。

【0108】本発明の他の実施例によれば、電話加入デ

ータの遠隔ローディング方法は複数のポアンテル契約者の間のROAMINGと称されるサービス（つまり、その独立局が加入していない補助的な電話ネットワークに対する呼び出し要求）にも適用される。

【0109】一般的に言って、ROAMINGサービスは、ポアンテル契約者に対する特別の加入を申し込んだ独立局の加入者に他のポアンテル契約者の補助的な交換ネットワークをある程度利用することを認めるものである。ここで、ROAMINGサービスは、その独立局に関するすべての公開および秘密データがその独立局のレベルと認証センターのレベルで同時に利用できる時のみ可能であることに注意すべきである。

【0110】他方、不正接続を避けるため、補助的交換ネットワークを運営する補助的認証センターはその独立局の電話加入データを持たない。

【0111】これまでのところ、独立局の加入者が補助的ネットワークの運営者との接続を確立するとき、補助的認証センターは認証センターから、ランダムワードと秘密キーによるその変換からなる1対の認証規格を要求している。秘密キーは通常独立局の秘密電話加入データ、例えば個人特定番号PINにより形成されている。

【0112】この1対の認証により独立局の補助センターレベルでの認証が可能である。

【0113】しかし、この認証方法による独立局の認証は次の理由で十分満足の行くものではない。

【0114】すなわち、一方では各認証センターのためのデータベースを形成するメモリーの間の通信はそれらが、各呼び出しの際、比較的長く、また体系的なものであるため、高い費用がかさむ。

【0115】他方、この認証方法は、独立局の認証を確認するためのデータベースを形成するメモリーを固定ターミナルが有する交換電話ネットワークには適切ではない。

【0116】出願人は、これらの不利な点を克服することのできる、ROAMINGサービスにおける電話加入データの遠距離ローディング方法を提供するという問題に直面した。

【0117】本発明によれば、図1および図4を参照して説明された発明に調和してコード化された秘密電話加入データPINを送信するという原理は、補助認証センターが独立局と補助交換電話ネットワークとの間の電話接続を認証するために必要なメインの認証センターから補助認証センターへの仮秘密電話加入データの送信に適用される。

【0118】このように、仮秘密電話加入データは送信の前に独立局のための特別キーの助けによりコード化される。特別キーが独立局とメインの認証センターに同時に格納されている秘密電話加入データPINから形成されるのは有利である。

【0119】図5には、独立局と独立局がそのための電

話加入データを有しない補助交換電話ネットワークとが相互電話通話をしている電話装置が略図的に示されている（いわゆるROAMINGサービス）。

【0120】独立局SPは補助電話装置と遠隔通話が可能である。この補助電話装置の主要構成要素は図1を参照して説明された電話装置のものと同一であり、同じ参照符号に添字Aを加えて示されている。

【0121】メイン認証センターCAは補助認証センターCAAと数値信号接続LCAAを介して接続されている。

【0122】ROAMINGサービスにおいては、電話加入データの遠隔ローディングは、メイン認証センターCAが補助認証センターCAAに数値信号接続LCAAを介して接続されているときだけ可能である。

【0123】電話加入データの遠隔ローディングは補助認証センターがメイン認証センターと協調して稼働しているときにのみ可能であることに注意すべきである。

【0124】図6には、ROAMINGサービスの枠組における仮秘密電話加入データの遠隔ローディングのプロトコルの主要な要素ステップが略図的に示されている。

【0125】ROAMINGサービスの枠組における遠隔ローディングのプロトコルの開始は、ここではステージE1R、E2RおよびE3Rから成り立っており、図3に言及して説明されたプロトコルの開始（ステージE1、E2、E3）と同一である。異なっているのは、電話呼び出し番号のフォーマットを囲むROAMINGキーボードの始動だけである。

【0126】独立局からの呼び出し要求（ステージE1R、E2RおよびE3R）の後、固定ターミナルは、補助認証センターにより運営される補助交換ネットワークと電話通信を確立するために認証要求を補助認証センターCAAに提出する（ステージE4R）。

【0127】ステージE4に関する電話通信を確立する許可の要求は図3を参照して説明された認証の要求に等しい（ステージE4R）。ROAMING情報の追加だけが異なっている。

【0128】補助認証センターが補助認証の問題であることを見いだせば、その補助認証センターは、独立局と補助交換電話ネットワークの間に電話接続を生成するためメイン認証センターからの許可を求めることを意図して認証要求を提出する。

【0129】補助認証センターからの認証要求（ステージE5R）に応じて、認証センターの制御手段は、まず第1に、それぞれ32ビットの値を持つ第1および第2のランダム数EPIN1およびEPIN2を生成する。

【0130】次に、認証センターのコード/デコード手段CDFは、暗号関数Fにより、（例えば本発明の方法による遠隔ローディングを通して駐在し、その機能を果たすため独立局のメモリーに格納された独立局の秘密電

話加入データを表す) 秘密キーPINの助けを得て、その第1および第2のランダム数EPIN1およびEPIN2のそれぞれの変換S1およびS2を計算する。

【0131】最後に、呼び出し要求のための公開数値ワードが独立局の認証に関する所定の条件を実証する時、認証センターの処理手段は変数データEPIN1およびEPIN2およびその変換S1およびS2の補助認証センターへの送信を許可する(ステージE6R)。

【0132】データEPIN1およびEPIN2、S1およびS2の送信に続いて、補助認証センターの制御手段MCFAは、公開仮電話加入データを生成し、それらを補助固定ターミナルBFAを介して独立局へと送信する。

【0133】さらに、制御手段MCFAは、64ビットのPRINを得るため変換S1と、変換S2に 2^{32} を掛けたものとの和の助けを得て、(秘密仮電話加入データを表す) 個人特定番号RPINを生成する(ステージE7R)。

【0134】場合により、制御手段MCFAは、やはり制御手段により生成され、上記の計算を排他的論理和により完成する、64ビットの値を持つ補足的変数データEPINの助けをさらに得て、PRINを生成する。

【0135】このように、一方では、補助認証手段のレベルにおける秘密仮データの生成が可能であるのは、変数ワードEPIN1およびEPIN2およびそれらの変換S1およびS2の送信による。他方、秘密仮電話加入データの遠隔ローディングが可能であるのは、補助手段と独立局間の変数ワードEPIN1、EPIN2および(場合により) EPIN3の送信による。

【0136】ワードEPIN1、EPIN2および(場合により) EPIN3の受け取りにより、独立局のコード/デコード手段は、第一に、秘密キーPINの助けを得て、暗号関数Fより、ワードEPIN1およびEPIN2のそれぞれの変換S1およびS2を計算する。最後にそれらは、秘密仮電話データPRINの回復のための計算に終わる(ステージE9R、E10R)。

【0137】最後に、このように受けとられた秘密でない仮公開電話加入データ、およびこのようにデコードされた秘密データはそれぞれのメモリーに格納される(ステージE10R)。

【0138】ステージE6の後、補助認証センターは、独立局の認証を可能にする仮秘密電話加入データRPINを有する。その結果、メイン認証センターによる補助認証センターの体系的な問い合わせはもはや必要ではな

い。

【0139】残りについては、補助認証センターによる独立局の認証に関するステージはメイン認証センターによる独立局の認証に関するステージと同一である。唯一の違いは、補助認証センターのレベルにおける仮公開電話加入データの生成にある。

【0140】補助認証手段が固定ターミナルに収納され、一般補助認証センターに接続されている場合は、本発明によれば、秘密仮電話加入データを補助認証手段のレベルで生成することを可能にするデータEPIN1、EPIN2、S1およびS2を受け取る目的のため、その固定ターミナルが一般補助認証センターを問い合わせる手段が備えられているようにすることができる。

【図面の簡単な説明】

【図1】本発明の電話装置の略図である。

【図2】本発明による電話加入データの遠隔ローディングに関するプロトコルを示す線図である。

【図3】本発明による独立局と固定ターミナル間のデータの交換を示す線図である。

【図4】秘密電話加入データのコード/デコードを示す線図である。

【図5】独立局が補助的交換電話ネットワークと相互に作用する本発明の電話装置を示す線図である。

【図6】図5の装置における、電話加入データの遠隔ローディングに関するプロトコルを示す線図である。

【符号の説明】

B F 固定ターミナル

C A 認証手段

C D F コード/デコード手段

C D P コード/デコード手段

E P I D 特別キー

L I D 呼び出し要求のための公開数値ワード

M C F 制御手段

M P F メモリー

M P P メモリー

M S F メモリー

M S P メモリー

P I D 独立局を特定するための公開数値ワード

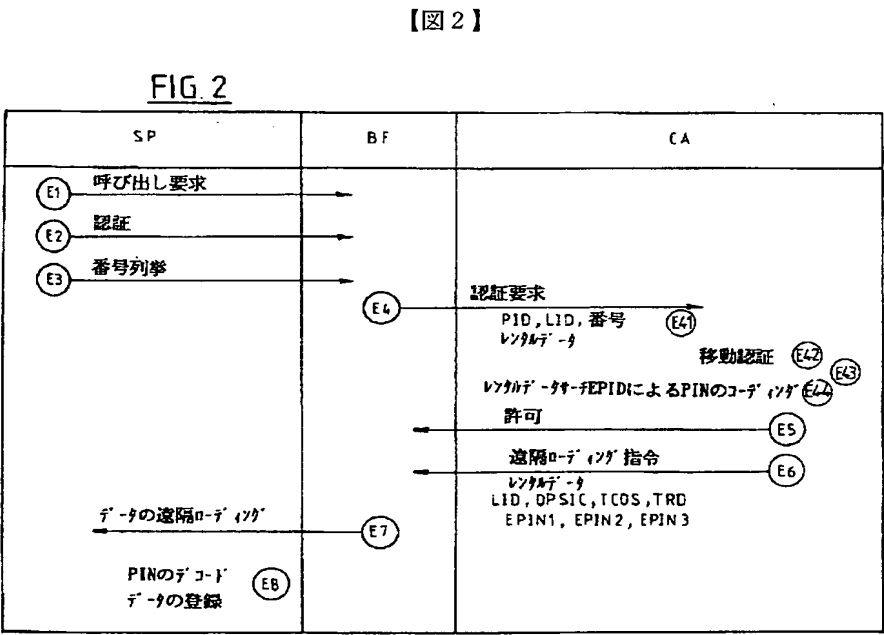
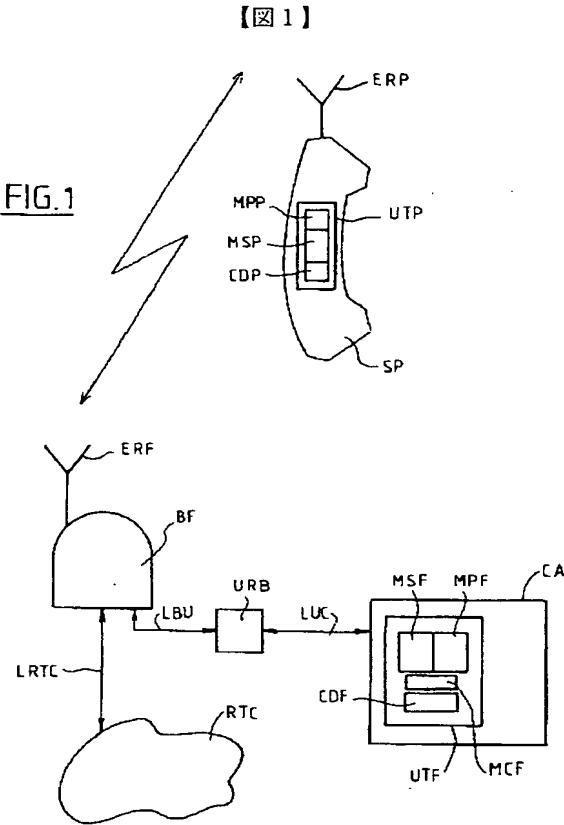
P I N 秘密特別キー

R T C 交換電話ネットワーク

S P 独立局

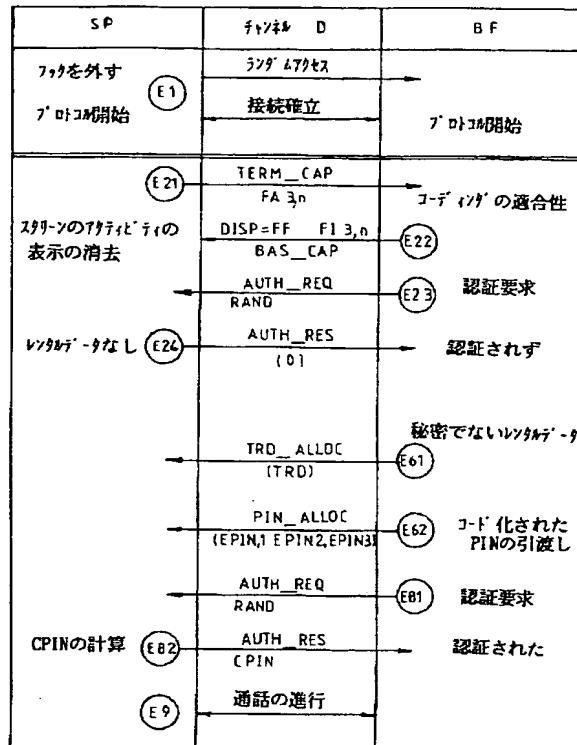
U T F 制御手段

U T P 処理手段

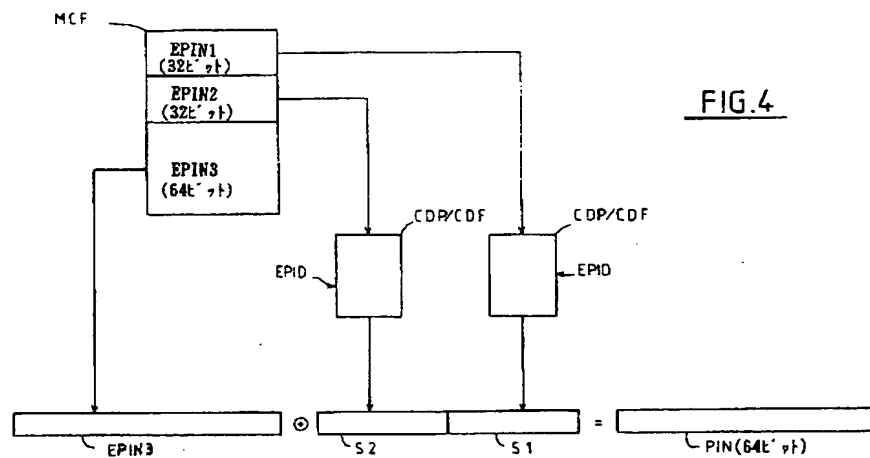


【図3】

FIG. 3



【図4】



[illegible]

```

sequenceDiagram
    participant SP
    participant BFA
    participant CAA
    participant CA

    SP->>BFA: E1R 呼び出し要求
    SP->>BFA: E2R 認証
    SP->>BFA: E3R 番号列挙
    BFA->>CAA: E4R 認証要求
    BFA->>CAA: PID LID 番号  
インタデータ
    CAA->>CA: E5R Roamingの検知
    CA->>CAA: E6R 許可
    CAA->>BFA: E7R RPINの計算  
EPIN3の生成
    BFA->>SP: E8R 遠隔ローピングの指令  
公開仮データ
    SP->>BFA: E9R 遠隔ローピング
    SP->>BFA: E10R RPINのデコード  
仮データの登録
  
```

FIG.6

(72)発明者 ソフィー・ボードゥ
フランス国、エフ-75013 パリ、リュ・
デ・コルデリエール、32